Trust in Merged ERP and Open Data Schemes in the "Cloud"

William Caelli
Queensland University of Technology, Australia
w.caelli@qut.edu.au

Vicky Liu
Queensland University of Technology, Australia
v.liu@qut.edu.au

She-I Chang
National Chung Cheng University, Taiwan
actsic@ccu.edu.tw

Abstract

Enterprise resource planning (ERP) systems are rapidly being combined with "big data" analytics processes and publicly available "open data sets", which are usually outside the arena of the enterprise, to expand activity through better service to current clients as well as identifying new opportunities. Moreover, these activities are now largely based around relevant software systems hosted in a "cloud computing" environment. However, the over 50-year old phrase related to mistrust in computer systems, namely "*garbage in, garbage out*" or "*GIGO*", is used to describe problems of unqualified and unquestioning dependency on information systems. However, a more relevant GIGO interpretation arose sometime later, namely "*garbage in, gospel out*" signifying that with large scale information systems based around ERP and open datasets as well as "big data" analytics, particularly in a cloud environment, the ability to verify the authenticity and integrity of the data sets used may be almost impossible. In turn, this may easily result in decision making based upon questionable results which are unverifiable. Illicit "impersonation" of and modifications to legitimate data sets may become a reality while at the same time the ability to audit any derived results of analysis may be an important requirement, particularly in the public sector. The pressing need for enhancement of identity, reliability, authenticity and audit services, including naming and addressing services, in this emerging environment is discussed in this paper. Some current and appropriate technologies currently being offered are also examined. However, severe limitations in addressing the problems identified are found and the paper proposes further necessary research work for the area.

(Note: This paper is based on an earlier unpublished paper/presentation *"Identity, Addressing, Authenticity and Audit Requirements for Trust in ERP, Analytics and Big/Open Data in a 'Cloud' Computing Environment: A Review and Proposal"* presented to the Department of Accounting and IT, College of Management, National Chung Chen University, 20 November 2013.)

I. INTRODUCTION - DEPENDENCE

"Garbage in, garbage out" (Wikipedia 2013), or "GIGO" is a term used to describe the problem of dependency on the output of computer based information systems. The phrase dates from the 1960s. However, a cynical version appeared later, namely *"garbage in, gospel out"*, which indicated that in large scale systems the ability to verify the accuracy of relevant data sets by their content is almost impossible. In addition the provenance and veracity of used software processing elements may also be totally unknown. So-called "big data" structures amplify this concern particularly where ERP systems and data analytics processes are combined and employed. This also means that trust must be placed in the naming and addressing structures employed to identify, access and thus depend upon the veracity of entities chosen, particularly in a "cloud computing" environment. Even in the physical world of cities, as their size and complexity expanded, the need for a scheme of naming and addressing became essential. Thus a highly dependable and trustworthy naming/addressing scheme for the elements involved in any information system is essential. This must include the computers, data storage, files/datasets, programs and network elements used. Moreover, these schemes must now cope with very large scale and complex but rapidly changing structures as well as their existence in national and international regulatory and enterprise requirements. Usually, both audit and forensic requirements exist. These normally involve retention of transaction details, associated metadata, etc., often necessitating the retention of the "traversal" undertaken by an application on behalf of a user. Moreover, that *"user"* may no longer be a human person but rather a *"thing"* as in the *"Internet-of-Things"* (Weber 2010) which is rapidly growing and objects of all types become interconnected and co-dependent. Such systems are being created around a combination of the Internet's data network protocol set with its associated hardware and software artifacts and *"virtual machine (VM)"* (Rosenblum and Garfinkel 2005) technology in the associated computers. These are then coupled with *"World Wide Web (WWW)"* based information handling processes.

This naming and addressing problem, as it relates to current usage of cloud computing environments, is summarised by Celesti et al (2010) as follows.

> *In cloud computing environments, as well as in all systems characterized by a high level of dynamism, naming and resource location become critical issues. Until now, the Internet has used the Domain Name System (DNS) for the resolution of domain names, that does not seem to be suitable to the new emerging cloud scenarios.*

However, equally critical is any associated identification and addressing scheme used within an actual computer, or virtual machine, employed which, in turn, must be mapped to from another system anywhere on the Internet. Celesti et al (2010) also state that in this environment *"…the need of an effective cloud naming system should be characterized by: scalability, extensibility, services of description and discovery, name recycling, non-correlation, and name space integration mechanisms which avoid name conflicts."*

However, in proposing that a new naming and addressing scheme is needed, they do not mention the critical importance of necessary trustworthiness and resilience with associated needs for reliable collection of audit and forensic data, including all necessary metadata.

II. OTHIS AND "REALMS"/REGIONS

The *"Open and Trusted Health Information Systems (OTHIS)"* project at the Queensland University of Technology clearly identified distinct *"realms"* vital to the identification and authentication of elements within an e-health system. In such *"realms"*, complementary naming and addressing schemes may be needed. Moreover, these schemes must be able to "mesh" together as required for a resource to be clearly and unambiguously identified, authenticated and accessed. These realms were identified (Liu 2011; Liu Caelli et al 2007a; Liu Caelli et al 2008a; Liu Caelli et al 2008b; Liu Caelli et al 2007b; Liu Caelli et al 2009a; Liu Caelli et al 2010; Liu Franco et al 2009b) as being:

- Health Informatics Access Control (HIAC),
- Health Informatics Application Security (HIAS), and
- Health Informatics Network Security (HINS).

The aim of the OTHIS project (Liu 2011; Liu et al 2007a; Liu et al 2009b) was:

> *... to address privacy and security requirements at each level within a modern HIS architecture to ensure the protection of data from both internal and external threats. OTHIS has the capacity to ensure legal compliance of any HIS to appropriate legislative and regulatory requirements.*

This research recognised that trustworthy naming, addressing and authentication of data and software processes had clear roles to play in any overall security design and assessment. It also recognised that the above *"realms"* concept may be generalized into extension of broader aspects of trusted/trustworthy *"access control"* including authentication and authorization (at the computer system level), application security (at the database and software process levels) and network security (at the data interconnection level). For example, it was identified by Henrickson et al (2007) and Croll et al (2007) that naming and resource location/authentication and access control in connected computer systems presented radically different approaches when *"Discretionary Access Control (DAC)"* were compared to *"Mandatory Access Control (MAC)"* structures provided by an operating system (Department of Defense 1985).

Naming, addressing and authentication, with associated audit and forensic services, of the entities in each of these realms have become critical security concerns. This also includes the vital aspect of trust in the systems that actually perform these naming, addressing and authentication processes. For usage of a *"public cloud"* environment, in particular, the situation takes on a new dimension in that the processes involved may themselves be virtualised and distributed over systems on a global basis.

III. NAMING AND ADDRESSING IN AN AGE OF *"CLOUD COMPUTING"*

"Cloud computing" systems are built upon much earlier naming and addressing schemes with associated and differing levels of assurance, from a public network environment to a closed computer system. A number of suggestions have therefore been suggested for an extension of these earlier schemes to address the cloud environment. These are largely based around extending the concepts of the *"Uniform Resource Locator (URL)"* associated with the World-Wide –Web (Davis and Reed ; Dong Yajuan et al 2006).

Earlier attempts at secure and manageable naming and addressing schemes include:

- the X.500 directory scheme for the *"Open Systems Interconnection (OSI)"* model proposed by the *International Telecommunications Union (ITU)*, coupled with the actual OSI model itself and its security standard (International Standard IS 7498-2);
- proprietary systems used for service identification in such network products as IBM's "System Network Architecture (SNA)", "Digital Equipment Corporation Network (DECNET), Novell Network scheme, NetBIOS from Microsoft, etc.;
- the "World-Wide-Web (WWW)" Uniform Resource Locator (URL) and allied URI/URN scheme;
- earlier "Data Dictionary (DD)" concepts and systems;
- current "Application Programming Interface (API)" structures for "Open Data" integration and,
- the current Internet *"Domain Name System (DNS)"* and its *"Domain Name System Security Extensions (DNSSEC)"*.

However, dependence now exists on the DNS which dates from around November 1983, over 30 years ago. This was also the same year that the newer Transmission Control Protocol/Internet Protocol (TCP/IP) protocol set replaced the earlier Network Control Program (NCP) protocol (Miller 2010). At the time, the Advanced Research Projects Agency Network (ARPANET) consisted of only some 68 nodes but rapid expansion was foreseen.

The scheme for the now Internet, then ARPANET, based naming and addressing structure grew out of the problem of maintaining and distributing a centralized file of relevant data (hosts.txt) as the then ARPANET expanded. The relevant RFC stated as follows (Mockapetris 1983):

> *As applications grow to span multiple hosts, then networks, and finally internets, these applications must also span multiple administrative boundaries and related methods of operation (protocols, data formats, etc). The number of resources (for example mailboxes), the number of locations for resources, and the diversity of such an environment cause formidable problems when we wish to create consistent methods for referencing particular resources that are similar but scattered throughout the environment.*

That Internet standard stated the problem as being one of a basic need for a *"consistent name space which will be used for referring to resources. In order to avoid the problems caused by ad hoc encodings, names should not contain addresses, routes, or similar information as part of the name."* However, this, and its related later standards, did not address the critical problem of security and resilience of the actual naming and addressing system as it took a central and critical role in the global Internet, particularly after 1988. A strict hierarchical naming form was proposed with an associated name to address resolution structure. Indeed RFC 882 (Mockapetris 1983) clearly stated that the overall plan was for a scheme whereby *"the domain name space is a tree structure."* This seemed appropriate at the time given the provenance of the then ARPANET and its management/control structures. Interestingly, it was not until some 14 years later that the problem of overall security of the DNS was considered via the *"Domain Name System Security Extensions (DNSSEC)"* RFC set. The basic DNSSEC RFC stated as follows (Eastlake and Kaufman 1997):

> *The Domain Name System (DNS) has become a critical operational part of the Internet infrastructure yet it has no strong security mechanisms to assure data integrity or authentication.*

The use of DNSSEC technology, and required hardware/software subsystems, is, however, limited and almost non-existent in the private sector. This is significant as globally stored datasets and software processes, often managed and controlled by third party system providers, become the norm and these are integrated into enterprise resource planning (ERP) systems which now encompass all management aspects of any large scale enterprise's activities, public or private. In this situation, private enterprise data sets may be combined with other, often "open", data sets from public or government sources, such as for planning market development activity, optimizing distribution and stocking schemes, managing supply chains, etc. A major research question is one of whether or not the DNSSEC architecture can be expanded to meet the new requirements for assured identification, addressing and authentication in a cloud computing environment combining multiple resources from highly varying sources. One extension of DNSSEC, the *"DANE"* proposal, from the *"DNS-based Authentication of Named Entities (DANE)"* working group of the Internet Engineering Task Force (IETF), sets out a proposition to answer this entity authentication need in the Internet as follows (Barnes 2012).

> *Authentication of domain names is a fundamental function for Internet security. In order for applications to protect information from unauthorized disclosure, they need to make sure that the entity on the far end of a secure connection actually represents the domain that the user intended to connect to.*

DANE proposes a new *"chain of trust"* that may be employed to increase confidence in data and programs used in a global Internet environment. However, this proposal does not extend below the *"network realm"*, as identified in OTHIS, to the authentication of the

individual assets within a real or virtual computer system that an ERP or data analytics system may use and depend upon.

At the same time the concept of *"Unified Communications (UC)"* (Riemer and Taing 2009) has developed. As the structure of the global telecommunications infrastructure rapidly changes, from the *"public switched telephone network (PSTN)"* (Liu and Ansari 2008) to *"packet switching"* technologies information services for any enterprise are being combined into a single, Internet protocol based facility, with such technologies as *"voice-over-internet protocol (VoIP)"* (Goode 2002) etc. Thus the Internet's DNS is coming under major pressure to incorporate these changes. This even further accentuated as enterprises, large and small, employ cloud computing incorporating both *"virtual machine (VM)"* and *"virtual network (VN)"* technologies. For example, the "private branch exchange (PBX)" (Muller 2002), offering traditional voice/switched circuit services, is being rapidly replaced by UC services. Almeida and Lourenco (2011) state that UC has the potential to improve enterprise communications and reduce business operating costs. However, Bradley and Shah (2010) outline no less than 11 major threats to the security of the UC environment, many of which involve trust in the naming and addressing scheme in use once the security of the earlier switched circuit system is removed. The International Telecommunications Union (ITU) "ENUM" (E.164) standard addresses this problem as indicated in a "Wikipedia" entry as follows.

> *Telephone number mapping is a system of unifying the international telephone number system of the public switched telephone network with the Internet addressing and identification name spaces. Internationally, telephone numbers are systematically organized by the E.164 standard, while the Internet uses the Domain Name System (DNS) for linking domain names to IP addresses and other resource information. Telephone number mapping systems provide facilities to determine applicable Internet communications servers responsible for servicing a given telephone number using DNS queries. The most prominent facility for telephone number mapping is the E.164 Number Mapping (ENUM) standard. It uses special DNS record types to translate a telephone number into a Uniform Resource Identifier (URI) or IP address that can be used in Internet communications.*

Van der Berg (2010) refers to this accelerating change and the need for nation states to carefully evaluate any transition from technical, control/management, legal and public policy aspects. The security requirements for any "ENUM" registry at a national level must be thoroughly analyzed. However, major research into this problem cannot be readily identified. Moreover, adoption of the ENUM standard has to first occur and it appears that, at present, few nations have moved in this direction. A database held by the RIPE ENUM group (Réseaux IP Européens) details the practical problems in adoption of this standard. For example, this report claims that for Australia any ENUM project is *"in hiatus"*, viz. not

progressing since *“ ... due to the current lack of interest in ENUM, a commercial implementation should not be established at this time.”* Similarly, for Taiwan as a further example, this report claims that *“although the User-ENUM domain for country code 886 has been delegated, no information for enumdata.org has yet been provided by the delegatee.”* However, in reality the adoption of VoIP and allied video services has rapidly progressed at the enterprise level, i.e. replacing the functions of the earlier PBX on the enterprise side. These security challenges need to be urgently addressed as any ENUM based national telecommunications structure develops.

IV. ERP, ANALYTICS AND “BIG/OPEN DATA” – CORRECT RESOURCES?

The above considerations, of course, apply to the “network realm” as identified in the OTHIS project (Liu 2011; Liu et al 2007a; Liu et al 2008a; Liu et al 2008b; Liu et al 2007b; Liu et al 2009a; Liu et al 2010; Liu et al 2009b) and normally do not address naming and addressing inside a host, or even a client, computer system, virtual or real, client or server. In the computer system case secure and reliable naming and addressing structures depend upon the level of granularity to be catered for. At a higher/system level, an appropriate file system holding both data and program entities, takes on this responsibility with protection of that “file structure” left to access control subsystems enforced by the operating system. At a next level, e.g. the “database” level, such structures as a “database schema” or associated “metadata” may identify the elements composing a database and their relationships. These entities may then be accessed by a name using, for example, a “query language” such as SQL or by direct named reference from an application program through an associated API.

In any enterprise environment employing ERP systems the situation in regard to trustworthy naming and addressing is rapidly becoming more complex. At one level, such as at an enterprise’s own individual ERP level, proprietary data sets employed are usually enterprise specific and protected under appropriate entity rule sets set out by the organisation. However, ERP today is making use of “external” datasets to develop appropriate business plans, e.g. national demographic data sets from governmental entities may be incorporated for the development of better business planning, etc. For example, human resource/personnel planning may draw upon open social networks such as “LinkedIN” as well as “in-house” data to enhance appropriate analysis of employment requirements, and so on. In turn, even larger scale or “big data” collected by the enterprise itself over time may be the subject of data analytics to further provide background for ERP activity.

The concept of a “data dictionary” was a common theme for many years as database technology gained widespread acceptance from the 1970s. It was defined as follows by IBM in 1993 (IBM Corporation 1993):

> *data dictionary n.*
>
> *A centralized repository of information about data such as meaning, relationships to other data, origin, usage, and format. It assists management, database*

administrators, system analysts, and application programmers in planning, controlling, and evaluating the collection, storage, and use of data.

A *"data dictionary (DD)"* (IBM Corporation 1993) contains all the necessary metadata needed to answer access requests but without any security requirements clearly defined. As discussed later, an enhanced data dictionary concept may be a candidate for the assurance needed for data and process entity access control and authentication needed in a cloud environment. However, this concept places a greater reliance on the trust and thus security of the data dictionary itself. This mirrors earlier concepts of a separate and verified access control sub-system as a vital part of any basic operating system design.

All of these processes make assumptions about the correctness of data/metadata used. In particular, where external data sets are used and relied upon the need to trust the provenance of those data sets is a paramount concern, as already alluded to. This concern now extends to the files or data sets that in the past were under strict control of the enterprise itself, through the support and maintenance of them on in-house computer and data network systems, but which now may reside on a public cloud computing service. She and Thursisingham (2007) have already affirmed that security is critical for ERP systems. However, with ERP related data moving to both private and public cloud systems environments earlier sureties have disappeared and trust must now be placed in the security of any cloud system, public or private, and its provider/operator.

V. THE "OPEN DATA" MOVEMENT – INTEGRATION INTO ERP / ANALYTICS – AUDIT AND FORENSICS NEEDS

Further candidates for the enhancement of security for naming, addressing, authentication and access control services in an emerging cloud computing environment may involve use of the technologies being employed in the *"open data"* movement. Essentially, the "open data" movement, now being embraced by government worldwide, sets out to make available the "raw" data held, but often closed, by public sector and other related enterprises. For example (see Figure 1), the State of Queensland, Australia, has now placed some 499 datasets onto an open server to encourage development of new software and services using that data (Queensland Government 2013) while the UK has placed 10,333 such datasets, as at October 2013, into its open data website.

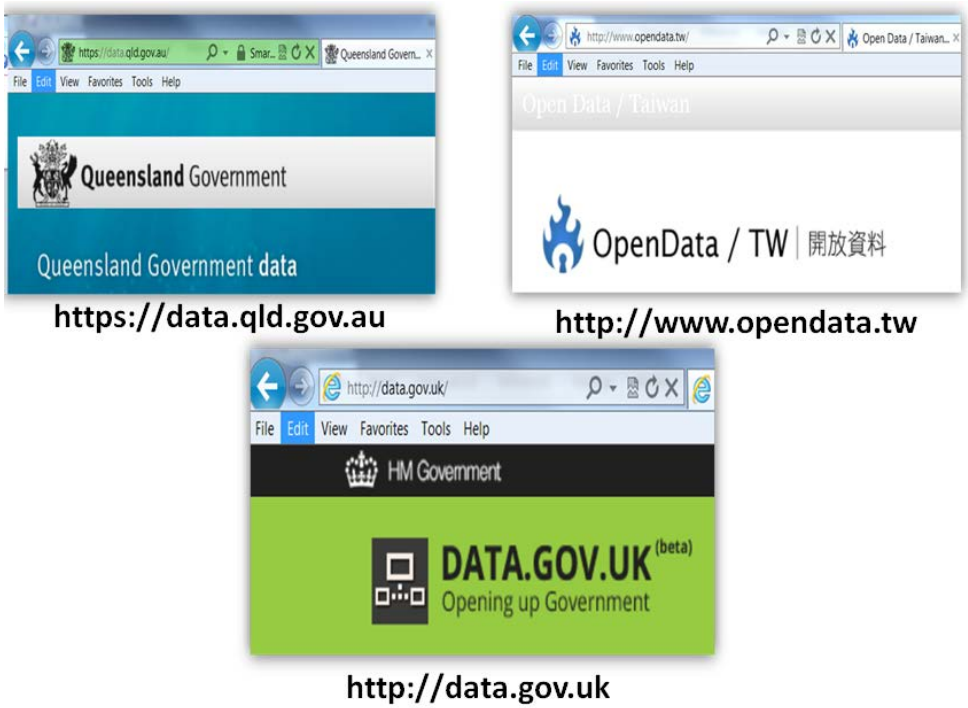

Figure 1. Websites for dataset provisioning.

The *"open data"* concept has been explained in a Wikipedia entry as "*the idea that certain data should be freely available to everyone to use and republish as they wish, without restrictions from copyright, patents or other mechanisms of control. The goals of the open data movement are similar to those of other "Open" movements such as open source, open hardware, open content, and open access. The philosophy behind open data has been long established (for example in the Mertonian tradition of science), but the term "open data" itself is recent, gaining popularity with the rise of the Internet and World Wide Web and, especially, with the launch of open-data government initiatives such as Data.gov and Data.gov.uk."* A key element of the "open data" (Miller Styles et al 2008) concept is that anyone may use offered datasets for any purpose free from onerous overriding restrictions but with some conditions that the provenance of the data is acknowledged and any passing on of the data via, say, an application is likewise unrestricted. However, software products incorporating such data may be offered for sale commercially. This is again emphasized by the appropriate definition given by the "Open Knowledge Foundation" (URL http://okfn.org/opendata/) which states that *"Open data is data that can be freely used, reused and redistributed by anyone – subject only, at most, to the requirement to attribute and sharealike."* The movement should be compared to, and be seen as an outgrowth of, similar activities such as the "open source" movement covering availability of software systems but with some notable differences in relation to software product sale commercially. However, the major problem to be solved is standardization for definition of necessary metadata structures. A complimentary research challenge is that of incorporation of appropriate integrity and authenticity checks into such metadata structures. Moreover, the necessity for such security enhancement of the

overall open data concept needs to be embraced and studied by associated public policy and legal entities.

The State of Queensland has offered prizes for applications that *"...demonstrate the most innovative use of and real outcomes from public data."* Similarly, in Taiwan, similar efforts to promote the "open data" cause have recently occurred through the formation of an alliance which was established in September 2013 following the earlier adoption of the open data cause by the Government of Taiwan. It is vital in this situation that the veracity of any dataset used can be tested prior to any major application development occurring along with trusted ongoing maintenance of the data set. Trust will be placed in any output from such applications given that such data may be readily and legally "re-published" with the associated software product. This may occur under an appropriate legal arrangement, such as through the *"Creative Commons"* concept. In the case of Queensland, the *"CKAN"* facility is used to enable access to datasets and elements. The CKAN facility, from the *"Open Knowledge Foundation"* is described as follows (Open Knolwedge Foundation).

> *CKAN is a powerful data management system that makes data accessible – by providing tools to streamline publishing, sharing, finding and using data. CKAN is aimed at data publishers (national and regional governments, companies and organizations) wanting to make their data open and available.*

It offers a range of facilities including an *"Application Programming Interface (API)"* for use by software developers but does not, at present, offer verification and any allied security mechanisms or services, similar to the proposals in the OSI security model, for example.

However, a number of alternatives and complimentary services and sub-systems exist, such as the *"Representational State Transfer (REST)"* scheme which has been defined as follows (Rodriguez 2008).

> *REST defines a set of architectural principles by which you can design Web services that focus on a system's resources, including how resource states are addressed and transferred over HTTP by a wide range of clients written in different languages. If measured by the number of Web services that use it, REST has emerged in the last few years alone as a predominant Web service design model.*

Once again, however, REST does not attempt to answer any underlying security concerns and, in fact, leaves these to the web servers involved via control and management of responses to requests.

Thus, research is urgently needed into the security mechanisms and services offered, planned to be offered or not offered at all, by these emerging "open data" service systems. A key question is one of whether or not they can be extended to meet the authentication and resilience needs of a comprehensive naming and addressing system operating in a global cloud computing environment.

At the same time, dependence on ERP results by any organisation dictates that appropriate audit records are maintained in case of dispute, legal/forensic needs or to further enhance opportunities. Such audit records are usually required in any legal "discovery" situation related to litigation or police investigation. Data, transactions, program/process invocation and metadata may all be elements whose access and usage need to be recorded in audit records even where records are created from both internal and external resources. At present there appears to be little to no consideration of these requirements in the technologies and sub-systems being developed or used. Legislative requirements may even exist that require such records to be created and stored for later analysis. The research problem here is one of elucidating and defining mechanisms for the identification and description of such requirements in such a way as to be able to include them in any data dictionary like structure used to provide a solution to the need along with the associated enforcement processes.

VI. CONCLUSIONS: RESEARCH DIRECTIONS IN TRUST FOR NAMING, ADDRESSING, AUTHENTICATION AND ACCESS CONTROL IN THE "CLOUD" FOR ERP/OPEN-BIG DATA

Research directions in the area of large scale systems for ERP and analytics in support of enterprise development must address the urgent need for new structures for reliable, scalable and secure/trusted naming and addressing schemes for entities maintained and accessed via a global Internet. Moreover, computational and data storage elements will be based, in many cases, around various forms of "cloud computing" (Armbrust Fox et al 2010) particularly for large private and public enterprises. At the same time, the "open data" movement has commenced and access to large public dataset collections will compliment usage of internal datasets used by an ERP system. At the same time, the need for high trust audit record creation and storage has accelerated with growing requirements being set out in legislative instruments at national and regional levels aimed at assisting in forensic accounting (Skalak Golden et al 2011) procedures.

A number of immediate research directions can be readily identified. These include:

- Provisioning of necessary and verifiable authentication and integrity controls in the metadata structures proposed for open data sets, potentially based on current markup-language schemes and any potential interaction with associated metadata schemes in use for proprietary ERP facilities;
- Incorporation of the DNSSEC (Domain Name System Security) architecture into access verification processes for both open data sets and closed ERP databases where application systems are involved;
- Implications of the movement to IPv6 structures, with associated IPSec and related facilities, for access to both proprietary ERP related and open datasets;
- Development of the concept of mandatorily enforced "profiles" in relation to access control parameters for ERP and open data systems;

- Clear identification of “realms” or sub-structures that can be independently managed and secured while maintaining an overall security posture, involving possible examination of the earlier “Open Systems Interconnection (OSI)” model security architecture espoused in international standard IS 7498-2 with its associated security mechanisms/services structure and layering concept;
- Definition of a security meta-structure that allow for security parameters that may radically differ from data set to data set and any associated programs/processes, e.g. from ERP related data to open data sets, that allows for disparate open data interfaces (APIs) to be used.

This paper has considered some candidate technologies for the comprehensive task of addressing security and trustworthiness requirements in ERP schemes incorporating both enterprise-controlled and open, third-party collections. More research, design, development, testing and experimentation are all required. Researchers need to define and build small demonstrator systems that may be used to clarify basic concepts and engineering/information system principles along with determination of appropriate design and implementation parameters. In addition, the usual performance and trustworthiness/security factors need to be incorporated. Any viable solution set must be implementable using currently accepted and understood information technology development and testing systems, usually based around the World-Wide-Web paradigm and an environment where end-user systems may be widely varied and of unknown security status. This requirement for new levels of overall information system security is, of course, exacerbated by the *“Bring-Your-Own-Device (BYOD)”* (Potts 2012) phenomenon, particularly when considering use of “big data” analytics techniques and enterprise ERP systems, along with “open data” from public sources, for the presentation of important, confidential and actionable results to enterprise management in both the public and private sectors. Overall, it appears that a new paradigm is required for the enhancement of the trustworthiness of an extended naming and addressing scheme for “cloud computing” based elements existing internationally connected to a globally connected Internet.

REFERENCES

1. Almeida, F., and Lourenço, J. 2011. "Security Issues in Unified Communications," *International journal of research and reviews in computer science* (2:2), p 403.
2. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., and Stoica, I. 2010. "A view of cloud computing," *Communications of the ACM* (53:4), pp 50-58.
3. Barnes, R. 2012. "Domain Name Authentication with DNSSEC and DANE," *The Internet Protocol Journal* (15).
4. Bradely, T., and Shah, S. 2010. *Unified Communications for Dummies*, Wiley Publishing Inc.

5. Celesti, A., Villari, M., and Puliafito, A. Year. "Ecosystem of Cloud Naming Systems: an Approach for the Management and Integration of Independent Cloud Name Spaces," Network Computing and Applications (NCA), 2010 Ninth IEEE International Symposium on Network Computing and Applications, IEEE Computer Society2010.
6. Croll, P., Henricksen, M., Caelli, W., and Liu, V. Year. "Utilizing SELinux to Mandate Ultra-secure Access Control of Medical Records," 12th World Congress on Health (Medical) Informatics, Medinfo2007, Brisbane Australia, 2007.
7. Davis, P., and Reed, D. "OASIS Extensible Resource Identifier (XRI)."
8. Department of Defense 1985. "Trusted Computer System Evaluation Criteria (TCSEC), USA 1983/1985, DoD 5200.28-STD Supersedes CSC-STD-00l-83, dated l5 Aug 83, Library No. S225,7ll, 26 December 1985 ".
9. Dong, Y., Yajuan, Q., Hongke, Z., Huachun, Z., and Bo, W. Year. "URNS: A new name service for uniform network resource location," Wireless, Mobile and Multimedia Networks, 2006 IET International Conference on2006, pp. 1-4.
10. Eastlake, D., and Kaufman, C. 1997. "Domain Name System Security Extensions."
11. Goode, B. 2002. "Voice over Internet protocol (VoIP)," *Proceedings of the IEEE* (90:9), pp 1495-1517.
12. Henricksen, M., Caelli, W., and Croll, P. Year. "Securing Grid Data Using Mandatory Access Controls," 5th Australian Symposium on Grid Computing and e-Research (AusGrid), Ballarat Australia, 2007.
13. IBM Corporation 1993. "Dictionary of IBM & Computing Technology."
14. Liu, J., and Ansari, N. 2008. *Public Switched Telephone Network*, John Wiley & Sons.
15. Liu, V. 2011. *An Architecture for Enhanced Assurance in E-Health Systems*, Queensland University of Technology, Brisbane.
16. Liu, V., Caelli, W., May, L., and Croll, P. Year. "A Sustainable Approach to Security and Privacy in Health Information Systems," 18th Australasian Conference on Information Systems (ACIS) Toowoomba, Australia, 2007a.
17. Liu, V., Caelli, W., May, L., and Croll, P. 2008a. "Open Trusted Health Informatics Structure," in *Australasian Workshop on Health Data and Knowledge Management, the Australian Computer Science Week* ACM: Wollongong Australia.
18. Liu, V., Caelli, W., May, L., and Croll, P. 2008b. "Strengthening Legal Compliance for Privacy in Electronic Health Information Systems: A Review and Analysis," *The Electronic Journal of Health Informatics (eJHI)* (Vol 3:1: e3).
19. Liu, V., Caelli, W., May, L., Croll, P., and Henricksen, M. 2007b. "Current Approaches to Secure Health Information Systems are Not Sustainable: an Analysis," in *12th World Congress on Health (Medical) Informatics, Medinfo*: Brisbane, Australia.
20. Liu, V., Caelli, W., May, L., and Sahama, T. Year. "Privacy and Security in Open and Trusted Health Information Systems," Third Australasian Workshop on Health Informatics and Knowledge Management (HIKM 2009), ACS, Wellington, New Zealand,

2009a, pp. 25-30.
21. Liu, V., Caelli, W., Smith, J., May, L., Lee, M., Ng, Z., Foo, J., and Li, W. Year. "Secure Architecture for Australia's Index Based E-health Environment " The Australasian Workshop on Health Informatics and Knowledge Management in conjunction with the 33rd Australasian Computer Science Conference Conferences in Research and Practice in Information Technology (CRPIT), Brisbane, Australia, 2010.
22. Liu, V., Franco, L., Caelli, W., May, L., and Sahama, T. Year. "Open and Trusted Information Systems/Health Informatics Access Control (OTHIS/HIAC)," the 32nd Australasian Computer Science Conference (ACSC 2009), ACS, Wellington, New Zealand, 2009b.
23. Miller, P. 2010. *TCP/IP - the Ultimate Protocol Guide: Complete 2 Volume Set* Brown Walker Press.
24. Miller, P., Styles, R., and Heath, T. Year. "Open Data Commons, a License for Open Data," LDOW2008.
25. Mockapetris, P. 1983. "RFC 882 Domain Names - Concepts and Facilities," Internet Engineering Task Force.
26. Muller, N. 2002. *Desktop Encyclopedia of Telecommunications*, McGraw-Hill.
27. Open Knolwedge Foundation "The open source data portal software."
28. Potts, M. 2012. "The state of information security," *Network Security* (2012:7), pp 9-11.
29. Queensland Government 2013. "Queensland Government data."
30. Réseaux IP Européens "RIPE ENUM Working group, ."
31. Riemer, K., and Taing, D.-I. S. 2009. "Unified Communications," *Business & Information Systems Engineering* (1:4), pp 326-330.
32. Rodriguez, A. 2008. "RESTful Web services: The basics," IBM.
33. Rosenblum, M., and Garfinkel, T. 2005. "Virtual machine monitors: current technology and future trends," *Computer* (38:5), pp 39-47.
34. She, W., and Thuraisingham, B. 2007. "Security for Enterprise Resource Planning Systems," *Information Systems Security* (16:3), pp 152-163.
35. Skalak, S. L., Golden, T. W., Clayton, M. M., and Pill, J. S. 2011. *A guide to forensic accounting investigation*, John Wiley & Sons.
36. Van der Berg, R. 2010. "ENUM: Dragging telephone numbers into the Internet Age."
37. Weber, R. H. 2010. "Internet of Things – New security and privacy challenges," *Computer Law & Security Review* (26:1), pp 23-30.
38. Wikipedia 2013. "Wikipedia, the free encyclopedia " in *Garbage in, garbage out*, Wikipedia.